THAT WHICH IS CLAIMED IS:

1. A method of generating RSA cryptographic values, the method comprising the steps of:

obtaining entity specific information (B) about a user;

obtaining a first secret seed value (W_p) and a second secret seed value (W_q);

obtaining a third, publicly known, randomization value (IV) having a first portion (IV_p) and a second portion (IV_q);

dividing a potential range of RSA encryption values into a first interval and a second interval;

generating a first initial value (XX_p) based on the first secret seed value (W_p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_p);

mapping the first initial value to an entity specific segment of the first interval utilizing the obtained entity specific information (B) to provide a mapped first initial value (X_p);

selecting a first entity dependent RSA cryptographic value (p) from the entity specific segment of the first interval utilizing the mapped first initial value as a starting point for a search for the first entity dependent RSA cryptographic value;

generating a second initial value (XX_q) based on the first entity dependent RSA cryptographic value (p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_q);

mapping the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information to provide a mapped second initial value (X_q); and

selecting a second entity dependent RSA cryptographic value (q) from the entity specific

segment of the second interval utilizing the mapped second initial value as a starting point for a search for the second entity dependent RSA cryptographic value.

2. A method according to Claim 1, further comprising the step of generating auxiliary prime divisors corresponding to the first entity dependent RSA cryptographic value (p) and the second entity dependent RSA cryptographic value (q).

3. A method according to Claim 2, wherein the auxiliary prime divisors are generated based upon the first secret seed value (W_p), the second secret seed value (W_q) and the third randomization value (IV).

4. A method according to Claim 3, wherein p_0 is a publicly known prime number whose length is at least n bits and g is a public generator, and wherein the step of generating auxiliary prime divisors comprises the steps of:

concatenating the first secret seed value (W_p), the second secret seed value (W_q) and the third randomization value (IV) so as to provide an exponent value (X);

determining an initial random value by determining $Y=g^X(\mathrm{mod}p_0)$;

selecting initial prime search values from the initial random value;

setting the most significant bit of the initial prime search values to "1" to provide final prime search values; and

selecting as the prime divisors the smallest prime value greater than or equal to the final prime search values.

5. A method according to Claim 4, further comprising the steps of:

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if the length of at least one of the prime divisors is greater than the length of the final prime search values; and

re-generating the prime divisors if the length of at least one of the prime divisors is greater than the length of the final prime search values.

6. A method according to Claim 4, wherein the initial prime search values have a first length if a public encryption exponent (*e*) has an odd value and a second length of the public encryption exponent (*e*) has an even value.

7. A method according to Claim 5, wherein the first length is 120 bits and the second length is 118 bits.

8. A method according to Claim 1, wherein the entity specific segments comprise the segments $[A+(B(C-A))/2^b, A+((B+1)(C-A))/2^b]$ wherein *A* and *C* are the endpoints of the respective intervals and the entity specific information comprises b bits.

9. A method according to Claim 8, wherein the RSA cryptographic values comprise n bits and wherein the first interval comprises RSA cryptographic values from the set of $[\sqrt{2}(2^{n-1}), 2^{n-1}+2^{n-3/2}]$ and the second interval comprises RSA cryptographic values from the set of $[2^{n-1}+2^{n-3/2}, 2^n]$.

10. A method according to Claim 9, wherein the binary size of the RSA cryptographic values are $2n$, a size m is n-b-2 and wherein the step of mapping the first initial value comprises the steps of:

linearly mapping the first initial value to a entity specific segment of the first interval utilizing the obtained entity specific information (B) utilizing the linear mapping function

$$G_{1,U}(x) = 4\left(1-\frac{1}{\sqrt{2}}\right)x+\sqrt{2}2^{n-1}+4\left(1-\frac{1}{\sqrt{2}}\right)(B-1)2^{m-1};\quad \text{and}$$

selecting as the mapped first initial value (X_p) the integer value which is not greater than the first initial value (XX_p) mapped utilizing the mapping function $G_{1,U}$; and

wherein the step of mapping the second initial value comprises the step of linearly mapping the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information (B) utilizing the linear mapping function $G_{2,U}(x) = 4\left(1-\frac{1}{\sqrt{2}}\right)x+2^{n-1}+2^{n-3/2}+4\left(1-\frac{1}{\sqrt{2}}\right)(B-1)2^{m-1}$;

selecting as the mapped second initial value (X_q) the integer value which is not greater than the second initial value (XX_q) mapped utilizing the mapping function $G_{2,U}$.

11. A method according to Claim 1, wherein the entity specific information is biometric information.

12. A method according to Claim 1, wherein the entity specific information is a globally unique user identification.

13. A method according to Claim 1, further comprising the steps of:

determining if a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval;

determining if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval; and

restarting the cryptographic value generation utilizing the first and second secret seed values and third randomization value if either a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval or if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval.

14. A method according to Claim 1 further comprising the steps of:

determining if $2^{16}-1$ candidates for p have been rejected in selecting the first entity dependent RSA cryptographic value;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if $2^{16}-1$ candidates for p have been rejected in selecting the first entity dependent RSA cryptographic value;

determining if $2^{16}-1$ candidates for q have been rejected in selecting the second entity dependent RSA cryptographic value;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if $2^{16}-1$ candidates for q have been rejected in selecting the second entity dependent RSA cryptographic value; and

restarting the cryptographic generation utilizing the first and second secret seed values and third randomization value if either $2^{16}-1$ candidates for p have been rejected in selecting the first entity dependent RSA cryptographic value or if $2^{16}-1$ candidates for q have been rejected in selecting the second entity dependent RSA cryptographic value.

15. A method according to Claim 1, wherein the step of generating a first initial value comprises the steps of:

mixing a concatenation of W_q and IV_q utilizing a publicly known mixing function;

concatenating W_p and IV_p; and

EXCLUSIVE-ORing the mixed concatenation of W_q and IV_q and the concatenation W_p and IV_p to provide the first initial value (XX_p); and

wherein the step of generating a second initial value comprises the steps of:

EXCLUSIVE ORing p and IV_p;

mixing the EXCLUSIVE OR of p and IV_p utilizing the publicly known mixing function;

concatenating W_q and IV_q; and

EXCLUSIVE-ORing the mixed EXCLUSIVE OR of p and IV_p and the concatenation of W_q and IV_q to provide the second initial value (XX_q).

16. A method according to Claim 1, further comprising the step of authenticating generated candidate RSA cryptographic values.

17. A method according to Claim 16, wherein the step of authenticating comprises the steps of:

recovering two candidate prime values utilizing the RSA public modulus (N) and the private signature exponent (d);

establishing a first of the two prime values as a first candidate cryptographic value (p') and the second of the two prime values as a second candidate cryptographic value (q');

recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV;

generating first and second RSA cryptographic values p'' and q'' utilizing W_p' and W_q' and IV; and

comparing p' and p'' and q' and q'' to authenticate the RSA cryptographic values.

18. A method according to Claim 17, further comprising the step of determining that the RSA cryptographic values are not authentic if p' and q' are values outside the entity defined segments of the first and second intervals.

19. A method according to Claim 17, wherein the first of the two prime numbers is a smaller of the two prime numbers.

20. A method according to Claim 17, wherein the step of recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV comprises the steps of:

inverse mapping the second candidate value q' to provide a first initial value S_q;

EXCLUSIVE ORing the first candidate cryptographic value p' and IV_p;

mixing the EXCLUSIVE OR of the first candidate cryptographic value p' and IV_p with the publicly known mixing function;

EXCLUSIVE ORing the mixed EXCLUSIVE OR of the first candidate cryptographic value p' and IV_p with IV_q to provide a first known value (N_q) having a length (j);

determining if a value corresponding to the j least significant bits of S_q is less than the first known value N_q;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the first candidate cryptographic value p' and IV_p with the n-j most significant bits of S_q if the value corresponding to the j least significant bits of the first subsequent value is not less than the first known value N_q, to provide the second candidate seed value;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the first candidate cryptographic value p' and IV_p with 1 subtracted from the value corresponding to the n-j most significant bits of S_q if the value corresponding to the j least significant bits of the first subsequent value is less

than the first known value N_q, to provide the second candidate seed value;

inverse mapping the first candidate value p' to provide a second initial value S_p;

concatenating the second candidate seed value and IV_q;

mixing the concatenation of the second candidate seed value and IV_q with the publicly known mixing function;

EXCLUSIVE ORing the mixed concatenation of the second candidate seed value and IV_q with IV_p to provide a second known value N_p having a length (j);

determining if a value corresponding to the j least significant bits of S_p is less than the second known value N_p;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatentation of the second candidate seed value and IV_q with the n-j most significant bits of S_p if value corresponding to the j least significant bits of the second subsequent value is not less than the second known value N_p, to provide the first candidate seed value;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the second candidate seed value and IV_q with 1 subtracted from the value corresponding to the n-j most significant bits of S_p if the value corresponding to the j least significant bits of the second subsequent value is less than the second known value N_p, to provide the first candidate seed value.

21. A method according to Claim 20, wherein j is 256 bits.

22. A system for generating an RSA cryptographic value, utilizing entity specific information (B) about an entity, a first secret seed value (W_p) and a second secret seed value (W_q), and a third, publicly known, randomization value (IV) having a first portion (IV_p) and a second portion (IV_q), comprising:

means for dividing a potential range of RSA encryption values into a first interval and a second interval;

means for generating a first initial value (XX_p) based on the first secret seed value (W_p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_p);

means for mapping the first initial value to a entity specific segment of the first interval utilizing the obtained entity specific information (B) to provide a mapped first initial value (X_p);

means for selecting a first entity dependent RSA cryptographic value (p) from the entity specific segment of the first interval utilizing the mapped first initial value as a starting point for a search for the first entity dependent RSA cryptographic value;

means for generating a second initial value (XX_q) based on the first entity dependent RSA cryptographic value (p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_q);

means for mapping the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information to provide a mapped second initial value (X_q); and

means for selecting a second entity dependent RSA cryptographic value (q) from the entity specific segment of the second interval utilizing the mapped second initial value as a starting point for a search

for the second entity dependent RSA cryptographic value.

23. A system according to Claim 22, further comprising means for authenticating generated candidate RSA cryptographic values.

24. A system according to Claim 23, wherein the means for authenticating comprises:

means for recovering two candidate prime values utilizing the RSA public modulus (n) and the private signature exponent (d) of the encrypted message;

means for establishing a first of the two prime values as a first candidate cryptographic value (p') and the second of the two prime values as a second candidate cryptographic value (q');

means for recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV;

means for generating first and second RSA cryptographic values p'' and q'' utilizing W_p' and W_q' and IV; and

means for comparing p' and p'' and q' and q'' to authenticate the message.

25. A computer program product for generating an RSA cryptographic value, utilizing entity specific information (B) about an entity, a first secret seed value (W_p) and a second secret seed value (W_q), and a third, publicly known, randomization value (IV) having a first portion (IV_p) and a second portion (IV_q), comprising:

a computer readable storage medium having computer readable program code embodied in said medium, said computer readable program code comprising:

computer readable code which divides a potential range of RSA encryption values into a first interval and a second interval;

computer readable code which generates a first initial value (XX_p) based on the first secret seed value (W_p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_p);

computer readable code which maps the first initial value to a entity specific segment of the first interval utilizing the obtained entity specific information (B) to provide a mapped first initial value (X_p);

computer readable code which selects a first entity dependent RSA cryptographic value (p) from the entity specific segment of the first interval utilizing the mapped first initial value as a starting point for a search for the first entity dependent RSA cryptographic value;

computer readable code which generates a second initial value (XX_q) based on the first entity dependent RSA cryptographic value (p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_q);

computer readable code which maps the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information to provide a mapped second initial value (X_q); and

computer readable code which selects a second entity dependent RSA cryptographic value (q) from the entity specific segment of the second interval utilizing the mapped second initial value as a starting

point for a search for the second entity dependent RSA cryptographic value.

26. A computer program product according to Claim 25, further comprising computer readable code which authenticates generated candidate RSA cryptographic values.

27. A computer program product according to Claim 26, wherein the computer readable code which authenticates comprises:

computer readable code which recovers two candidate prime values utilizing the RSA public modulus (n) and the private signature exponent (d) of the encrypted message;

computer readable code which establishes a first of the two prime values as a first candidate cryptographic value (p') and the second of the two prime values as a second candidate cryptographic value (q');

computer readable code which recovers first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV;

computer readable code which generates first and second RSA cryptographic values p'' and q'' utilizing W_p' and W_q' and IV; and

computer readable code which compares p' and p'' and q' and q'' to authenticate the message.